JOURNAL OF COMBINATORIAL THEORY, Series A **72**, 345–350 (1995)

Note

On a Problem of Hering Concerning Orthogonal Covers of $\mathbf{K}_n$*

A. GRANVILLE

University of Athens, Athens, Georgia

H.-D. O. F. GRONAU

Universität Rostock, Rostock, Germany

AND

R. C. MULLIN

University of Waterloo, Waterloo, Ontario, Canada

Communicated by the Managing Editors

Received October 12, 1994

A Hering configuration of type k and order n is a factorization of the complete digraph $\mathbf{K}_n$ into n factors each of which consists of an isolated vertex and the edge-disjoint union of directed k-cycles, which has the additional property that for any pair of distinct factors, say $\mathbf{G}_i$ and $\mathbf{G}_j$, there is precisely one pair of vertices, say $\{a, b\}$, such that $\mathbf{G}_i$ contains the directed edge (a, b) and $\mathbf{G}_j$ contains the directed edge (b, a). Clearly a necessary condition for a Hering configuration is $n \equiv 1 \pmod k$. It is shown here that for any fixed k, this condition is asymptotically, and, it is shown to be always sufficient for $k = 4$. © 1995 Academic Press, Inc.

1. INTRODUCTION

Let $n \geqslant 1$ be an integer and let $\mathbf{K}_n$ denote the complete digraph on the n-element vertex set V. We consider collections $\mathscr{G} = \{\mathbf{G}_1, \mathbf{G}_2, ..., \mathbf{G}_n\}$ of spanning subdigraphs of $\mathbf{K}_n$. Note that the number of digraphs in $\mathscr{G}$ coincides with the size of V. We call $\mathscr{G}$ an *orthogonal cover* of $\mathbf{K}_n$ if

(i) every directed edge of $\mathbf{K}_n$ belongs to exactly one of the $\mathbf{G}_i$'s, and

* Research supported in part by NATO Grant CRG 940085.

0097-3165/95 $12.00

(ii) for every two subdigraphs $\mathbf{G}_i$ and $\mathbf{G}_j (i \neq j)$ there is a unique pair $\{a, b\}$ of vertices such that $\mathbf{G}_i$ contains the directed edge (a, b) and $\mathbf{G}_j$ contains the directed edge (b, a).

Since the number of members of $\mathscr{G}$ equals the number of vertices, we can use the vertex set V to index the members of $\mathscr{G}$. Since each $\mathbf{G}_i$, $i \in V$ is spanning, we can consider the vertex in $\mathbf{G}_i$ to be distinguished, and we will refer to i as the root vertex (or simply the root) of $\mathbf{G}_i$. Then we refer to $\mathbf{G}_i$ as being the *ith page* of the cover. Furthermore, $\mathbf{G}_i$ is said to be *idempotent* if the vertex i occurs as an isolated vertex in $\mathbf{G}_i$. The cover $\mathscr{G}$ is said to be *idempotent* if every page of $\mathscr{G}$ is idempotent. Note that every page must have exactly $n-1$ edges.

Hering [6] raised the question of determining, for a fixed integer $k \geqslant 3$, for which values of n does there exist an orthogonal cover of $\mathbf{K}_n$ in which every page consists of an isolated vertex and a vertex disjoint union of directed cycles of length k. Such an configuration will be called a Hering configuration of type k and order n.

Clearly a necessary condition for the existence of a Hering configuration of type k, defined on $\mathbf{K}_n$, is that $n \equiv 1 \pmod{k}$. Let $S_k = \{n$: there exists a Hering configuration of type k and order $n\}$. It will be shown that for each integer $k \geqslant 3$, there exists an integer N_k such that if $n \equiv 1 \pmod{k}$ and $n \geqslant N_k$, then $n \in S_k$.

2. Constructions

In this section we discuss two constructions for Hering configurations, one of which is direct, and the other recursive.

THEOREM 2.1. *Let k be an integer, $k \geqslant 3$. Suppose that n is a prime power such that $n \equiv 1 \pmod{k}$. Then there exists a Hering configuration of type k and order n.*

Proof. Let $GF(n)$ denote the finite field of order n. Since $n \equiv 1 \pmod{k}$, there exists a kth root of unity β in $GF(n)$. Define a quasigroup $Q = (GF(n), o)$ by $xoy = \beta x + (1-\beta) y$ for $x, y \in GF(n)$. Then Q is idempotent, that is $xox = x$, for all $x \in GF(n)$. Also

$$\underbrace{(\cdots((xoy)\, oy)\cdots)\circ y)}_{k \text{ times}}$$
$$= \underbrace{\beta(\beta \cdots \beta x + (1-\beta)\, y) + (1-\beta)\, y)\cdots) + (1-\beta)\, y}_{k \text{ times}}$$
$$= \beta^k x + (\beta^{k-1} + \beta^{k-2} + \cdots + \beta + 1)(1-\beta)\, y$$
$$= \beta^k x + (1-\beta^k)\, y = x,$$

since β is a kth root of unity. Further, for a given pair of elements x and y, there exists a unique element u such that $(uox)\, oy = u$. Given these facts, it is easily verified that by defining $\mathbf{G}_i$ by

$$\mathbf{G}_i = \{(i)\} \cup \bigcup_{\substack{x \in GF(n) \\ x \neq i}} \{(x, xoi)\}$$

for $i \in GF(n)$, a Hering configuration of type k and order n is obtained. ∎

For the recursive construction, the notion of pairwise balanced design (PBD) is required. Let v be a positive integer, and K a subset of the positive integers. Then a pairwise balanced design $PBD[v, K]$ is a pair $(V, \mathscr{F})$ where V is a v-set and $\mathscr{F}$ is a family of subsets (called blocks) of v which satisfies the following:

(i) every pair of distinct elements of V occur in precisely one block;

(ii) the cardinality (size) of every block lies in K.

A set S of positive integers is said to be PBD-closed if it has the property that the existence of a PBD$[v, S]$ implies that v lies in S. A well known theorem of R. M. Wilson [9] states that a PBD-closed set S is ultimately periodic with period $\alpha = GCD\{s(s-1) : s \in S\}$.

THEOREM 2.2. *Let k be a fixed integer $\geqslant 3$. Then the set $S_k = \{n :$ there exists a Hering configuration of type k and order $n\}$ is PBD-closed.*

Proof. It is shown in [4] that if there exists a PBD $[n, S]$ and for each $s \in S$ there exists an idempotent orthogonal covering of $\mathbf{K}_s$, then there exists an idempotent orthogonal covering of $\mathbf{K}_n$ whose pages each consist of the idempotent together with vertex disjoint unions of the connected components, apart from the idempotents, of the pages of the covering $\mathbf{K}_s$. In the case at hand, these components are all directed cycles of length k, so the resulting configuration is a Hering configuration of type k and order n. Therefore S_k is PBD-closed. ∎

3. Asymptotic Results on the Sets $\mathscr{S}_k$

In this section, we show that for fixed $k \geqslant 3$, there exists an integer N_k such that if $n \equiv 1 \pmod k$ and $n \geqslant N_k$, then there exists a Hering configuration of type k and order n. To this end, let k be any integer, $k \geqslant 2$, and let $P(k) = \{p : p$ is a prime, $p \equiv 1 \pmod{k}\}$, and let $Q(k) = \{q : q = p^t$, p is a prime, t is a positive integer, $q \equiv 1 \pmod{k}\}$. For any non-empty set of positive integers S let $\beta(S) = GCD\{s(s-1) : s \in S\}$.

LEMMA 3.1. *Let k be an integer, $k \geqslant 2$. Then there exist two primes p_1 and p_2 in $P(k)$ such that $GCD(p_1(p_1-1), p_2(p_2-1)) = 2k$.*

Proof. By Dirichlet's Theorem on primes in an arithmetic progression (see [1]), there exists a prime p_1 such that $p_1 \equiv 1 \pmod{2k}$, say $p_1 = 1 + 2ka$ for some positive integer a. Further by Dirichlet's theorem there exists a prime p_2 such that $p_2 \equiv 1 + 2k \pmod{2kp_1 a}$, say $p_2 = 1 + 2k + 2kp_1 ab$ for some positive integer b. Note that $p_2 > p_1$. Therefore

$$\begin{aligned} GCD(p_1(p_1-1), p_2(p_2-1)) &= GCD(p_1(p_1-1), p_2-1) \\ &= GCD(p_1 2ka, 2k + 2kp_1 ab) \\ &= 2kGCD(p_1 a, 1 + p_1 ab) \\ &= 2k, \end{aligned}$$

as required. ▮

COROLLARY 3.1.1. *Let k be an integer, $k \geqslant 3$. Then*

(i) *$\beta(P(k))$ divides $2k$.*

(ii) *Further if k is even, then $\beta(P(k)) = k$.*

Proof. Part (i) is a direct consequence of Theorem 3.1 and the definition of $\beta(P(k))$. For part (ii), assume that k is even, that is, $k = 2s$ where $s > 2$. By Theorem 3.1, there exist primes p_1 and p_2 in $P(s)$ such that $GCD(p_1(p_1-1), p_2(p_2-1)) = 2s = k$. But p_1 and p_2 are both odd and they are both relatively prime to s, since they lie in $P(s)$. Hence $2s$ divides both $p_1 - 1$ and $p_2 - 1$, so p_1 and p_2 are in $P(k)$.

These are then the required primes. ▮

These results can be applied to the sets S_k as follows.

THEOREM 3.2. *Let k be any integer, $k \geqslant 3$. Then there exists a constant N_k such that if $n \geqslant N_k$ and $n \equiv 1 \pmod{k}$, then $n \in S_k$.*

Proof. By Theorem 2.1, we have $P(k) \subset Q(k) \subset S_k$, so S_k is non-empty and $k \leqslant \beta(S_k) \leqslant 2k$, with $\beta(S_k) = k$ if k is even.

Wilson's theory states that the PBD-closed set S_k is ultimately periodic with period $\beta(S_k)$, and that for any m in S_k there exists a constant C_m such that if $n \geqslant C_m$ and if $n \equiv m \pmod{\beta(S_k)}$, then $n \in S_k$. We consider two cases, namely k odd and k even. Suppose first that k is even. Then $\beta(S_k) = k$, and since S_k contains some member $m \equiv 1 \bmod k$, then by Wilson's theorem there exists a constant N_k as in the enunciation of this theorem.

Now consider the case when k is odd. Then the argument is slightly more difficult, since in this case $\beta(S_k) = 2k$. Now suppose that $m \equiv 1 \bmod k$. If m is odd, then $m \equiv 1 \pmod{2k}$, and if m is even, then $m \equiv k+1 \pmod{2k}$. Therefore if we can show that S_k contains both odd and even integers, an argument similar to that above applied to each of these cases will establish the existence of the required integer N_k. But since k is odd, then $2^{\phi(k)} \equiv 1 \pmod{k}$ where $\phi(k)$ is the Euler phi function, so $2^{\phi(k)} \in Q(k)$. Therefore S_k contains both odd and even integers, and the theorem follows. ∎

4. The Spectrum of Hering Configurations of Type 4

Ganter and Gronau [2] have shown that $S_3 = \{n : n \geq 4,\ n \equiv 1 \pmod 3),\ n \neq 10\}$. To obtain an analogous result for S_4, we require the notion of the closure of a set of positive integers. Let K be any nonempty set of positive integers. Then $B[K] = \{n : \text{there exists a } PBD[n, K]\}$ is clearly PBD closed and is called the closure of K.

It is shown in [5] and [7] that $B[\{5, 9, 13, 17, 29, 33\}] = \{n : n \geq 5,\ n \equiv 1 \pmod 4)\}$. But $\{5, 9, 13, 17, 29\}$ is a set of prime powers, and a Hering configuration of type 4 and order 33 is exhibited in Table I. Therefore $S_4 = \{n : n \geq 5,\ n \equiv 1 \pmod 4)\}$.

For $k = 5$, an exhaustive search shows that there is no Hering configuration of type 5 and order 6. However such configurations exist for $n = 11$ and 16 by Theorem 2.1. Examples of Hering configurations of type 5 and orders 21 and 26 are exhibited in Table II. However, with present methods a complete determination of $H(5)$ appears to be well beyond reach.

The case of Hering configurations of type 6 is much more complete because of the fact that so many early members of S_6 are primes and prime powers. Let $N(6) = \{n : n \geq 7,\ n \equiv 1 \pmod 6)\}$, and $C(6) = B[Q(6)]$. It is shown in [8] and [10] that $C(6) \supseteq N(6) \backslash E$ where $E = \{55, 115, 145, 205, 235, 253, 265, 295, 319, 355, 391, 415, 445, 451, 493, 649, 655, 667, 685, 697, 745, 781, 799, 805, 1243, 1255, 1315, 1585, 1795, 1819, 1921\}$.

This result was improved by Greig [3] who showed that $\{295, 655, 1243, 1255, 1795, 1819, 1921\} \subset C(6)$. Therefore there exists a Hering

TABLE I

A Hering Configuration of Type 4 and Order 33

$\{(0)\ (1, 2, 4, 3)\ (5, 8, 12, 19)\ (6, 28, 20, 16)\ (7, 31, 15, 25)$
$(9, 22, 10, 30)\ (11, 27, 24, 17)\ (13, 21, 26, 32)\ (14, 23, 18, 29)\} \pmod{33}$

TABLE II

A Hering configuration of type 5 and order 21

$\{(0)\,(1, 2, 4, 7, 12)\,(3, 18, 13, 19, 16)\,(5, 17, 10, 14, 6)$
$(8, 15, 11, 9, 20)\}\ (\text{mod } 21)$

A Hering configuration of type 5 and order 26

$\{((0, 0)), ((1, 0), (2, 0)\,(3, 0), (0, 1)), ((5, 0), (8, 0)\,(6, 0), (10, 0), (1, 1)),$
$((7, 0), (2, 1), (11, 0), (12, 1), (7, 1)), ((9, 0), (8, 1)\,(4, 1), (9, 1)\,(11, 1)),$
$((12, 0), (6, 1)\,(5, 1), (3, 1)\,(10, 1))\}$

$\{((0, 1)), ((0, 0)\,(5, 0)\,(12, 0)\,(7, 0)\,(7, 1)), ((11, 0), (4, 0), (1, 0), (10, 0), (3, 1)),$
$((6, 0), (4, 1), (3, 0), (8, 1), (9, 1)), ((8, 0), (10, 1)\,(2, 0), (11, 1), (1, 1)),$
$((9, 0), (12, 1), (5, 1), (2, 1), (6, 1))\}\ (\text{mod } 13, -).$

configuration of type 6 for all $n \in N(6)$ with the possible exception of $n \in \{55, 115, 145, 205, 235, 253, 265, 319, 355, 391, 415, 445, 451, 493, 649, 667, 685, 697, 745, 781, 799, 805, 1315, 1585, 1795\}$.

References

1. L.E. Dickson, "Theory of Numbers," Vol. 1, p. 415, Chelsea.
2. B. Ganter and H.-D. O. F. Gronau, On two conjectures of Demetrovics, Füredi, and Katona on partitions, *Discrete Math.* **88** (1991), 149–155.
3. M. Greig, Designs from projective planes and PBD bases, and designs from configurations in projective planes, preprint.
4. H. D. O. F. Gronau, R. C. Mullin, and P. J. Schellenberg, On orthogonal double covers of K_n and a conjecture of Chung and West, *J. Combin. Designs*, accepted for publication.
5. A. M. Hamel, W. H. Mills, R. C. Mullin, Rolf Rees, D. R. Stinson, and J. Yin, The spectrum of $PBD(\{5, k^*\}, v)$ for $k = 9$, 13, *Ars Combinatoria* **36** (1993), 7–26.
6. F. Hering, Balanced pairs, *Ann. of Discrete Math.* **20** (1984), 177–182.
7. E. R. Lamken, W. H. Mills, and R. M. Wilson, Four pairwise balanced designs, *Designs, Codes and Cryptography* **1** (1991), 63–68.
8. R. C. Mullin and D. R. Stinson, Pairwise balanced designs with block sizes $6t+1$, *Graphs and Combinatorics* **3** (1987), 365–377.
9. R. M. Wilson, An existence theory for designs. II. The structure of PBD-closed sets and the existence conjectures, *J. Combin. Theory* **13** (1972), 246–273.
10. Z. Zhu and D. Cheng, Orthogonal Steiner triple systems of order $6m+1$, unpublished manuscript.